

Department of Energy

§ 710.9

classified or sensitive information technology systems.

(h) An illness or mental condition of a nature which, in the opinion of a psychiatrist or licensed clinical psychologist, causes or may cause, a significant defect in judgment or reliability.

(i) Refused to testify before a Congressional Committee, Federal or state court, or Federal administrative body, regarding charges relevant to eligibility for DOE, or another Federal agency's access authorization.

(j) Been, or is, a user of alcohol habitually to excess, or has been diagnosed by a psychiatrist or a licensed clinical psychologist as alcohol dependent or as suffering from alcohol abuse.

(k) Trafficked in, sold, transferred, possessed, used, or experimented with a drug or other substance listed in the Schedule of Controlled Substances established pursuant to section 202 of the Controlled Substances Act of 1970 (such as marijuana, cocaine, amphetamines, barbiturates, narcotics, etc.) except as prescribed or administered by a physician licensed to dispense drugs in the practice of medicine, or as otherwise authorized by Federal law.

(l) Engaged in any unusual conduct or is subject to any circumstances which tend to show that the individual is not honest, reliable, or trustworthy; or which furnishes reason to believe that the individual may be subject to pressure, coercion, exploitation, or duress which may cause the individual to act contrary to the best interests of the national security. Such conduct or circumstances include, but are not limited to, criminal behavior, a pattern of financial irresponsibility, conflicting allegiances, or violation of any commitment or promise upon which DOE previously relied to favorably resolve an issue of access authorization eligibility.

[59 FR 35185, July 8, 1994, as amended at 66 FR 47063, Sept. 11, 2001]

§ 710.9 Action on derogatory information.

(a) If the reports of investigation of an individual or other reliable information tend to establish the validity and significance of one or more items in the criteria, or of other reliable information or facts which are of security

concern, although outside the scope of the stated categories, such information shall be regarded as derogatory and create a question as to the individual's access authorization eligibility.

(b) If a question arises as to the individual's access authorization eligibility, the Local Director of Security shall authorize the conduct of an interview with the individual, or other appropriate actions, which may include a DOE-sponsored mental evaluation, and, on the basis of the results of such interview or actions, may authorize the granting of the individual's access authorization. If, in the opinion of the Local Director of Security, the question as to the individual's access authorization eligibility has not been favorably resolved, he shall submit the matter to the Manager with a recommendation that authority be obtained to process the individual's case under administrative review procedures.

(c) If the Manager agrees that unresolved derogatory information is present and that appropriate attempts to resolve such derogatory information have been unsuccessful, he shall notify the Director, Office of Safeguards and Security, of his proposal to conduct an administrative review proceeding, accompanied by an explanation of the security concerns and a duplicate Personnel Security File. If the Manager believes that the derogatory information has been favorably resolved, he shall direct that access authorization be granted for the individual. The Manager may also direct the Local Director of Security to obtain additional information in the matter prior to deciding whether to grant the individual access authorization or to submit a request for authority to conduct an administrative review proceeding. A decision in the matter shall be rendered by the Manager within 10 calendar days of its receipt.

(d) Upon receipt of the Manager's notification, the Director, Office of Safeguards and Security, shall review the matter and confer with the Manager on:

(1) The institution of administrative review proceedings set forth in §§ 710.20 through 710.32;

§ 710.10

10 CFR Ch. III (1–1–02 Edition)

(2) The granting of access authorization; or

(3) Other actions as the Director deems appropriate.

(e) The Director, Office of Safeguards and Security, shall act pursuant to one of these options within 30 calendar days of the receipt of the Manager's notification unless an extension is granted by the Director, Office of Security Affairs.

[66 FR 47063, Sept. 11, 2001]

§ 710.10 Suspension of access authorization.

(a) If information is received that raises a question concerning an individual's continued access authorization eligibility, the Local Director of Security shall authorize action(s), to be taken on an expedited basis, to resolve the question pursuant to § 710.9(b). If the question as to the individual's continued access authorization eligibility is not resolved in favor of the individual, the Local Director of Security shall submit the matter to the Manager with a recommendation that the individual's access authorization be suspended pending the final determination resulting from the procedures in this subpart.

(b) Within two working days of receipt of the recommendation from the Local Director of Security to suspend the individual's DOE access authorization, the Manager shall review the matter and authorize continuation or suspension of access authorization. The access authorization of an individual shall not be suspended except by the direction of the Manager. This authority to suspend access authorization may not be delegated but may be exercised by a person who has been designated in writing as Acting Manager.

(c) Upon suspension of an individual's access authorization pursuant to paragraph (b) of this section, the individual, the individual's employer, any other DOE Operations Office having an access authorization interest in the individual, and, if known, any other government agency where the individual holds an access authorization, security clearance, or access approval, or to which the DOE has certified the individual's DOE access authorization, shall be notified immediately. The Cen-

tral Personnel Clearance Index shall also be updated. Notification to the individual shall be made in writing and shall reflect, in general terms, the reason(s) why the suspension has been effected. Pending final determination of the individual's eligibility for access authorization from the operation of the procedures provided in this subpart, the individual shall not be afforded access to classified matter, special nuclear material, or unescorted access to security areas that require the individual to possess a DOE access authorization.

(d) Following the decision to suspend an individual's DOE access authorization, the Manager shall immediately notify the Director, Office of Safeguards and Security, of the action and the reason(s) therefore. In addition, the Manager, within 10 calendar days of the date of suspension, shall notify the Director, Office of Safeguards and Security, of his proposal to conduct an administrative review proceeding, accompanied by an explanation of its basis and a duplicate Personnel Security File.

(e) Upon receipt of the Manager's notification, the Director, Office of Safeguards and Security, shall review the matter and confer with the Manager on:

(1) The institution of administrative review procedures set forth in §§ 710.20 through 710.32;

(2) The reinstatement of access authorization; or

(3) Other actions as the Director deems appropriate.

(f) The Director, Office of Safeguards and Security, shall act pursuant to one of these options within 30 calendar days of the receipt of the Manager's notification unless an extension is granted by the Director, Office of Security Affairs.

[59 FR 35185, July 8, 1994, as amended at 66 FR 47064, Sept. 11, 2001]

ADMINISTRATIVE REVIEW

§ 710.20 Purpose of administrative review.

These procedures establish methods for the conduct of the administrative